

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

BROIDY CAPITAL
MANAGEMENT LLC, *et al.*,

Plaintiffs,

v.

NICHOLAS D. MUZIN, *et al.*,

Defendants.

No. 19-cv-0150 (DLF)

MEMORANDUM OPINION

Plaintiffs Broidy Capital Management, LLC (BCM) and Elliott Broidy (together, “Broidy”) brought this suit against several foreign agents of Qatar: Nicolas Muzin, Joseph Allaham, Gregory Howard, and Stonington Strategies, LLC (a company founded by Muzin and Allaham). First Am. Compl. (“Complaint”), Dkt. 18 ¶¶ 11–18. Broidy alleges that the defendants joined a “Qatari Enterprise,” which conspired against him to hack his computers and disseminate the hacked information to the media in retaliation for Broidy’s anti-Qatari advocacy. *Id.* ¶¶ 1–2, 199. He brings thirteen counts against each of the defendants alleging violations of both federal and California law. Before the Court are Muzin and Stonington’s Motion to Dismiss the First Amended Complaint, Dkt. 40; Howard’s Motion to Dismiss the First Amended Complaint, Dkt. 41; and Allaham’s Motion to Dismiss the First Amended Complaint, Dkt. 42. For the reasons that follow, the Court will grant in part and deny in part the defendants’ motion to dismiss.

I. BACKGROUND

A. The Parties

Plaintiff Elliott Broidy is an outspoken critic for the State of Qatar and its sponsorship of terrorist organizations. Complaint ¶ 1. He resides in California and is the Chief Executive Officer for BCM, a California corporation with its principal place of business in Los Angeles. *Id.* ¶ 11.

The defendants are U.S. citizens and agents of Qatar. *Id.* ¶¶ 13–18. Muzin resides in Maryland and serves as the CEO for Stonington, a public relations consulting firm based in Washington D.C. and organized under the laws of Delaware. *Id.* ¶¶ 13, 18. On August 24, 2017, Muzin was retained by Qatar for consulting services. *Id.* ¶ 15. Stonington registered under the Foreign Agents Registration Act (FARA) as a foreign agent for Qatar on September 3. *Id.* ¶ 18.

Allaham is a New York resident and the co-founder of Stonington. *Id.* ¶ 16. He frequently conducts business for Stonington in D.C. and has worked for Qatar as a foreign agent. *Id.* Allaham originally worked as an unregistered foreign agent, until he filed a belated registration statement under FARA in response to a subpoena from Broidy on June 15, 2018. *Id.* ¶¶ 16, 69.

Howard is a Maine resident and media placement expert who worked at Conover & Gould (Conover), a firm based in D.C. *Id.* ¶ 17. He worked as a registered foreign agent of Qatar through Conover from July 2017 through January 18, 2018. *Id.* Howard now works as a Vice President for another D.C.-based public strategy firm, Mercury Public Affairs. *Id.*

B. Broidy Critiques Qatar

In June 2017, several neighboring Middle Eastern states severed diplomatic relations with Qatar and imposed an economic blockade and embargo against the country because of its support

for terrorism and close ties to Iran. *Id.* ¶ 42. The international sanctions were supported by the United States and have hurt the Qatari economy. *Id.* ¶ 43. Beginning in early 2017, Broidy became a vocal critic of Qatar’s support for terrorists and friendly relationship with Iran. *Id.* ¶ 46. He has regularly conveyed his criticism in meetings with United States officials, and on the issue of Qatari terrorism, he directly conferred with the President of the United States. *Id.* ¶ 47. The President criticized Qatar in a June 2017 meeting of the Republican National Committee, and during that meeting he stated to the audience: “Elliott Broidy is fantastic.” *Id.* ¶¶ 48–49. Broidy’s theory is that Qatar has formed a “Qatari Enterprise” with the chief goal of ending the sanctions against Qatar—in part by improving Qatar’s reputation in the United States. *Id.* ¶¶ 50–51. Targeting Broidy in response to his criticism was allegedly part of this effort. *Id.* ¶¶ 73–77.

C. Qatar Hires the Defendants

In the fall of 2017, Muzin and Allaham began working for Qatar alongside Jamal Benomar. *Id.* ¶ 53. Benomar coordinated payments from Qatar to Muzin and Allaham. *Id.* ¶ 54. In late August 2017, the Qatari Embassy officially retained Stonington and Muzin to influence public opinion regarding Qatar. *Id.* ¶ 55. Allaham also began working for Qatar in 2017 for the Emir of Qatar, Sheikh Tamim bin Hamad Al Thani, and his brother, Sheikh Mohamad bin Hamad Al Thani. *Id.* ¶ 56. Benomar was in close contact with Muzin and Allaham, holding approximately fifty phone calls over the relevant time period and establishing a group chat for the three of them to talk about business. *Id.* ¶ 76.

Muzin admitted to Broidy’s associate, Joel Mowbray, that he identified and described Broidy as an impediment to Qatar in his weekly meetings at the Qatari Embassy. *Id.* ¶¶ 73–74. Muzin stated that “Broidy’s name comes up in Embassy meetings often,” and Muzin “definitely

identified [Broidy] as somebody who, was not, didn't like them too much.” *Id.* ¶ 75. Muzin further admitted that his Qatari clients “knew about [Broidy]” and “knew that [Broidy] had been influential in shaping the White House’s views on Qatar.” *Id.*

D. BCM’s Servers Are Hacked

Starting in January 2018, Broidy and the BCM servers were hacked, allegedly by international cyber security firm Global Risk Advisors (GRA). *Id.* ¶¶ 77–78. On information and belief, Broidy believes that the Qatari Enterprise retained GRA for the hack, that GRA opened a subsidiary in Qatar, and that GRA knew the cyber hack was done for the benefit of Qatar. *Id.* ¶¶ 79–85. In laying the groundwork for the ultimate hack, hackers targeted Broidy’s spouse Robin Rosenzweig with a spear phishing email on December 27, 2017 and gained control of her Gmail account on or around January 3, 2018. *Id.* ¶¶ 86–90. They then did the same to Broidy’s executive assistant on or around January 14, 2018. *Id.* ¶¶ 91–95. Further, the hackers unsuccessfully targeted Mowbray around that time. *Id.* ¶ 96.

BCM has an exchange server physically located in Los Angeles, California. *Id.* ¶ 97. Hackers gained access to this server on January 16, 2018 and maintained unauthorized access to the BCM email server until at least February 25, 2018. *Id.* ¶¶ 98–99. Some of those hacking attempts came from Qatar and others were allegedly masked by VPN connections. *Id.* ¶¶ 100–06. Broidy alleges that other outspoken critics of Qatar have been targeted by the hacking scheme as well. *Id.* ¶ 108–09. On March 13, 2018, Allaham wrote to Muzin that “Benomar had gone to Qatar prior to the date of the message ‘to get the emails. That [sic] what I think he was doing there [in Qatar].’” *Id.* ¶ 111. Muzin responded by referencing Broidy by name. *Id.*

E. The Hacked Materials are Disseminated

From January 18, 2018 through May 22, 2018, Howard had extensive contacts with both

members of the Qatari Enterprise and reporters working on stories about Broidy that were based on materials stolen from the BCM servers. *Id.* ¶¶ 115, 119. Phone records show that he was in close and consistent contact with reporters before they began publishing stories about Broidy. *Id.* ¶¶ 117, 119–133. Between March 1, 2018 and May 21, 2018, stories about Broidy based on the stolen emails appeared in the *Wall Street Journal*, *New York Times*, the Associated Press, *Bloomberg*, *McClatchy*, and the *Huffington Post*. *Id.* ¶¶ 121, 123, 126, 141–42, 144, 152.

Meanwhile, and shortly after the cyberattack on January 25, Muzin sent Allaham a message stating “It’s very good. . . . We got the press going after Broidy. I emailed you.” *Id.* ¶ 140. While Muzin was in Qatar that day, a reporter from *McClatchy* reached out to Muzin about a story they were working on regarding Broidy. *Id.* ¶ 141. Muzin forwarded the message to Allaham and commented, “Time to rock.” *Id.* On February 28, Muzin called Mowbray and informed him that the *Times* was about to publish a story about Broidy and George Nader, saying that he received this information from his “media guy.” *Id.* ¶ 145. Broidy believes that Muzin’s “media guy” is Howard. *Id.* ¶ 146. On March 13, Muzin messaged Allaham to say that recent news stories about Broidy have “[p]ut[] him in [M]ueller[’s] crosshairs.” *Id.* ¶ 147. The next day, Muzin also told Allaham that he’d “get some intel about the Broidy event soon,” likely referring to a March 13 Republican fundraiser where Broidy was listed as an event host. *Id.* ¶ 149. On March 15, Muzin messaged Allaham, “Elliott Broidy was not at the fundraiser!” *Id.* ¶ 150. Finally, on May 4, following another Qatari agent’s meeting with a *Wall Street Journal* reporter, Muzin told Allaham that “our new friends can make Broidy go away altogether.” *Id.* ¶¶ 153–56.

F. The Defendants Are Paid and Continue to Talk

Muzin received a total of \$3.9 million in September and October 2017 from an alter ego

of Qatar, BlueFort Public Relations, LLC. *Id.* ¶¶ 161–63. Of that \$3.9 million, Muzin gave \$2.3 million to Allaham for “services rendered.” *Id.* ¶ 164. Muzin then received a pay raise from Qatar that coincided with the timing of the cyberattack, and Broidy alleges that Muzin and Allaham’s total compensation of over \$7 million from Qatar “far exceed[s] the prevailing market rates for lobbying or political action.” *Id.* ¶¶ 165–69.

Between February 27, 2018 and March 8, 2018, Muzin met with Mowbray on three separate occasions. *Id.* ¶ 171–72. During the first of those meetings, Muzin demonstrated foreknowledge of impending news stories about Broidy. *Id.* ¶¶ 174–76.

During the second meeting on March 5, he stated that there was “a lot more coming” from the *Times* and that Broidy was “in deep shit.” *Id.* ¶ 178. Muzin further stated that “there may be hacking stuff in there,” and that “‘it’s possible’ that Qatar had hacked his own phone and email accounts, and in fact that ‘it’s possible they try to hack people.’” *Id.* ¶ 179. He told Mowbray that, regarding his association with Broidy: “‘Honestly, you should be a little bit concerned about this. . . . You should (have a lawyer) because you’re very well-known and influential’ as someone with an ‘anti-Qatar’ position.” *Id.* ¶ 182.

Finally, in the third meeting, Muzin admitted to Mowbray that “Broidy’s name comes up in Embassy meetings often” and “I definitely identified him as somebody who . . . didn’t like them too much.” *Id.* ¶ 184. “Muzin further acknowledged that everyone he ‘fingered’ was ‘in danger,’” and that Qatar had “assembled an enemies list of people who were considered ‘hurdles’ to Qatar’s interests.” *Id.* He warned Mowbray that Mowbray and Broidy needed “to be very careful,” that Qatar is “going after you,” and that “‘Honestly, I know they’re after you and Broidy.’” *Id.* When Mowbray challenged Muzin regarding his knowledge of the information that could be known only through access to the illegally obtained emails, Muzin at first stated he got

his information from the “Dark Web.” *Id.* ¶ 187. “When Mowbray told Muzin that he suspected Muzin had helped initiate the cyber operation against Mr. Broidy, Muzin stated, ‘I was doing my job.’” *Id.* Muzin then stated that he needed “to be a little more careful” when he spoke to Mowbray. *Id.* And when Mowbray “asserted that Muzin was ‘neck deep in this conspiracy’ against Mr. Broidy, Muzin replied, ‘I know.’” *Id.*

G. This Case Begins

This is the third lawsuit that Broidy has brought against members of the Qatari Enterprise. The first was brought against Muzin, Qatar, and several other individuals in the Central District of California. *Id.* ¶ 189. The district court dismissed the lawsuit against Qatar on foreign sovereign immunity grounds and dismissed the suit as to all other defendants for lack of personal jurisdiction. *See generally Broidy Capital Mgmt., LLC v. State of Qatar*, No. CV 18-2421-JFW(Ex), 2018 U.S. Dist. LEXIS 226540 (C.D. Cal. Aug. 8, 2018); 2018 U.S. Dist. LEXIS 230853 (C.D. Cal. Aug. 16, 2018); 2018 U.S. Dist. LEXIS 230971 (C.D. Cal. Aug. 22, 2018). Broidy then brought a second suit against Jamal Benomar in the Southern District of New York, which was dismissed on grounds of diplomatic immunity. Complaint ¶ 190. Broidy then brought this third suit, alleging thirteen counts under federal statutes, California statutes, and California common law:

- Count I: RICO violations. *Id.* ¶¶ 192–258.
- Count II: Conspiracy to violate RICO. *Id.* ¶¶ 259–65.
- Count III: Violations of the Stored Communications Act. *Id.* ¶¶ 266–73.
- Count IV: Violations of the Computer Fraud and Abuse Act. *Id.* ¶¶ 274–88.
- Count V: Misappropriation of trade secrets in violation of the Defend Trade Secrets Act. *Id.* ¶¶ 289–307.
- Count VI: Misappropriation of trade secrets in violation of the California Uniform Trade Secrets Act. *Id.* ¶¶ 308–320.

- Count VII: Receipt and possession of stolen property. *Id.* ¶¶ 321–29.
- Count VIII: Violation of the California Comprehensive Computer Data Access and Fraud Act. *Id.* ¶¶ 330–40.
- Count IX: Public disclosure of private facts. *Id.* ¶¶ 341–49.
- Count X: Intrusion upon seclusion. *Id.* ¶¶ 350–56.
- Count XI: Conversion. *Id.* ¶¶ 357–67.
- Count XII: Tortious interference. *Id.* ¶¶ 362–67.
- Count XIII: Civil conspiracy. *Id.* ¶¶ 368–75.

Broidy seeks damages and injunctive relief against the four American defendants—Muzin, Howard, Allaham, and Stonington. *See id.* ¶¶ 192–375.

II. LEGAL STANDARDS

Federal Rule of Civil Procedure 12(b)(1) allows a defendant to dismiss a plaintiff’s complaint for lack of subject-matter jurisdiction. Foreign-official immunity is a question of subject-matter jurisdiction, *see Doe I v. Buratai*, 318 F. Supp. 3d 218, 226 (D.D.C. 2018), and a defendant “bears the burden of proving” it, *Lewis v. Mutond*, 918 F.3d 142, 145 (D.C. Cir. 2019). In evaluating a motion to dismiss under Rule 12(b)(1), the court must “assume the truth of all material factual allegations in the complaint and ‘construe the complaint liberally, granting plaintiff the benefit of all inferences that can be derived from the facts alleged.’” *Am. Nat’l Ins. Co. v. FDIC*, 642 F.3d 1137, 1139 (D.C. Cir. 2011) (quoting *Thomas v. Principi*, 394 F.3d 970, 972 (D.C. Cir. 2005)). But “‘the court need not accept factual inferences drawn by plaintiffs if those inferences are not supported by facts alleged in the complaint, nor must the Court accept plaintiff’s legal conclusions.’” *Disner v. United States*, 888 F. Supp. 2d 83, 87 (D.D.C. 2012) (quoting *Speelman v. United States*, 461 F. Supp. 2d 71, 73 (D.D.C. 2006)). The court “is not limited to the allegations of the complaint,” *Hohri v. United States*, 782 F.2d 227, 241 (D.C. Cir.

1986), *vacated on other grounds*, 482 U.S. 64 (1987), and “may consider such materials outside the pleadings as it deems appropriate to resolve the question whether it has jurisdiction to hear the case.” *Scolaro v. D.C. Bd. of Elections & Ethics*, 104 F. Supp. 2d 18, 22 (D.D.C. 2000) (citing *Herbert v. National Academy of Sciences*, 974 F.2d 192, 197 (D.C. Cir. 1992)).

Federal Rule of Civil Procedure 12(b)(6) permits a defendant to likewise dismiss a plaintiff’s complaint for failure to state a claim upon which relief can be granted. To survive such a motion, the complaint must contain “a short and plain statement of the claim showing that the pleader is entitled to relief, in order to give the defendant fair notice of what the claim is and the grounds upon which it rests.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (internal quotation marks and citations omitted). That is, the complaint “must contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 570). The job of evaluating a claim’s plausibility is “a context-specific task that requires the reviewing court to draw on its judicial experience and common sense.” *Iqbal*, 556 U.S. at 679. In evaluating a 12(b)(6) motion, “the Court need not accept inferences drawn by plaintiff if those inferences are not supported by the facts set out in the complaint, nor must the court accept legal conclusions cast as factual allegations.” *Hettinga v. United States*, 677 F.3d 471, 476 (D.C. Cir. 2012); *see Iqbal*, 556 U.S. at 678. But it must be sure to “construe the complaint in favor of the plaintiff, who must be granted the benefit of all inferences that can be derived from the facts alleged.” *Hettinga*, 677 F.3d at 476 (internal quotation marks omitted). A complaint that “ha[s] not nudged the[] claims across the line from conceivable to plausible” should be dismissed. *Twombly*, 550 U.S. at 570.

III. ANALYSIS

Defendants raise both jurisdictional and merits challenges to each of Broidy's claims. The Court rejects the defendants' jurisdictional argument. On the merits, the Court will deny in part and grant in part the defendants' motions.

A. Sovereign Immunity

The defendants move to dismiss under Rule 12(b)(1) for lack of subject matter jurisdiction. They argue that, as agents of Qatar, they are immune from suit. This issue “is properly governed by the common law,” not by the Foreign Sovereign Immunities Act (FSIA), because this case does not involve “a claim against a foreign state as the Act defines that term.” *Samantar v. Yousuf*, 560 U.S. 305, 325 (2010); *see also Lewis*, 918 F.3d at 145 (noting that when a “case involves foreign officials—not foreign states—the issue of immunity is governed by the common law”). The parties agree. *See* Stonington Mem. at 12–23, Dkt. 40-1; Howard Mem. at 1, Dkt. 41-1; Allaham Mem. at 1, Dkt. 42-1; Pls.' Opp. at 30, Dkt. 43.

“The doctrine of common law foreign immunity distinguishes between two types of immunity: status-based and conduct-based immunity.” *Lewis*, 918 F.3d at 145. “Status-based immunity is reserved for diplomats and heads of state and attaches regardless of the substance of the claim.” *Id.* (internal quotation omitted). It is unavailable here because the defendants are neither Qatari diplomats nor Qatari heads of state. “Conduct-based immunity,” on the other hand, “is afforded to any public minister, official, or agent of the state with respect to acts performed in his official capacity if the effect of exercising jurisdiction would be to enforce a

rule of law against the state.”¹ *Lewis*, 918 F.3d at 145 (internal quotation omitted) (alterations adopted).

The Supreme Court in *Samantar* outlined “a two-step procedure” for determining when defendants are “entitled to conduct-based foreign sovereign immunity.” *Lewis*, 918 F.3d at 145. At step one, “a foreign official requests a ‘suggestion of immunity’ from the State Department and, if granted, the District Court is divested of its jurisdiction.” *Id.* (quoting *Samantar*, 560 U.S. at 311). The State Department has not granted a suggestion of immunity to any defendant here, so the Court proceeds to step two. At step two, the Court considers “whether the defendants “satisfy the requisites for conduct-based immunity.” *Id.* at 146.

To date, neither the D.C. Circuit nor the Supreme Court has identified precisely how a court should determine whether the defendants have satisfied these requisites. The plaintiff identifies two possibilities. One possibility is that the Court must determine whether it is “the established policy of the State Department to recognize” the asserted “ground of immunity.” *Samantar*, 560 U.S. 310 at 312 (alteration adopted) (quotation omitted) (explaining that this was the relevant inquiry before the FSIA was enacted).

A second possibility is that the Court should apply the test found in Restatement § 66(f). This test considers three factors: “First, whether the actor is a public minister, official, or agent of the foreign state. Second, whether the acts were performed in her official capacity. And third, whether exercising jurisdiction would serve to enforce a rule of law against the foreign state.” *Lewis*, 918 F.3d at 146. The D.C. Circuit has applied this test to conclude that defendants

¹ The *Lewis* court drew this definition from the Restatement (Second) of Foreign Relations Law § 66(f) (1965) (“Restatement”). See 918 F.3d at 145. Though the *Lewis* court assumed without deciding that the Restatement is the proper test to apply at step two of the *Samantar* procedure, the *Lewis* court appears to have accepted the Restatement’s definition of conduct-based immunity.

lacked immunity. *Id.* at 148 (Srinivasan, J., concurring). And the Supreme Court has “previously found [the Restatement] instructive” on issues of foreign immunity. *Samantar*, 560 U.S. at 321.

That said, the D.C. Circuit in *Lewis* merely assumed “without deciding” that “Restatement § 66 captures the contours of common-law official immunity” because “both parties assume[d]” so. *Lewis*, 918 F.3d at 146; *cf. id.* at 148–49 (Randolph, S.J., concurring) (doubting that § 66 embodies common law and speculating that “[i]t may well be that there is not now and never was any common law of immunity for foreign officials sued in the United States.” *Id.* at 148–49 (Randolph, S.J., concurring). And the Supreme Court has “expressed no view on whether Restatement § 66 correctly sets out the scope of common-law immunity applicable to current or former foreign officials.” *Samantar*, 560 U.S. at 321 n.15.

Given this hesitation surrounding the Restatement, the Court will apply both the State Department test and the Restatement test to decide “whether the defendants “satisfy the requisites for conduct-based immunity.” *Lewis*, 918 F.3d at 146. The Court need not resolve which of the two tests properly applies because the defendants lack immunity under either test.

I. State Department Test

It is not the established policy of the State Department to recognize immunity for these defendants. In *Yousuf v. Samantar*, on remand from the Supreme Court, the State Department cited the defendant’s “status as a permanent legal resident” as a “major basis” for “submit[ing] a suggestion of non-immunity” for the defendant. 699 F.3d 763, 777 (4th Cir. 2012). The State Department explained that “U.S. residents . . . who enjoy the protections of U.S. law ordinarily should be subject to the jurisdiction of the courts, particularly when sued by U.S. residents.” *Id.* The State Department has recognized this principle elsewhere too. *See* United States Department of State Office of Foreign Missions, *Diplomatic and Consular Immunity: Guidance for Law*

Enforcement and Judicial Authorities 12 (2018), available at https://www.state.gov/wp-content/uploads/2019/07/2018-DipConImm_v5_Web.pdf (“Consular employees and consular service staff who are U.S. nationals, legal permanent residents, or who are permanently resident in the United States enjoy no personal inviolability or jurisdictional immunity in the United States.”).

Under this policy, the State Department would not recognize immunity for these defendants. Each individual defendant is a U.S. citizen who resides in the United States. Stonington, the lone corporate defendant, is organized under Delaware law and based in Washington, D.C. The plaintiff is a U.S. citizen bringing claims under domestic law—federal and state—for actions allegedly committed on United States soil. The defendants do not identify any examples of the State Department recognizing immunity in these circumstances.

The defendants have identified three out-of-circuit cases in which courts have extended foreign sovereign immunity to U.S. citizens. *See Butters v. Vance Int’l, Inc.*, 225 F.3d 462, 466–67 (4th Cir. 2000); *Ivey v. Lynch*, No. 1:17CV439, 2018 U.S. Dist. LEXIS 133656, at *20 (M.D.N.C. Aug. 8, 2018); *Alicog v. Kingdom of Saudi Arabia*, 860 F. Supp. 379, 384 (S.D. Tex. 1994), *aff’d*, 79 F.3d 1145 (5th Cir. 1996). But these cases are nonbinding and unpersuasive.

Turning first to *Butters*, in that pre-*Samantar* decision, the Fourth Circuit extended the “privilege” of *domestic* derivative sovereign immunity—*i.e.*, immunity for agents of the U.S. government—“to the private agents of foreign governments.” *Butters*, 225 F.3d at 466. The defendants argue that this doctrine of foreign derivative immunity is distinct from foreign-official immunity and should apply here.

A fundamental problem with this argument is that the D.C. Circuit has never adopted foreign derivative immunity as a distinct doctrine. To the contrary, the D.C. Circuit has

suggested that the common law of foreign immunity includes two, and only two, doctrines: status-based immunity and conduct-based immunity. *Lewis*, 918 F.3d at 145.

In addition, the rationale behind immunity for agents of the U.S. government does not necessarily apply to foreign agents. The rationale for domestic derivative sovereign immunity is that the United States and agents of the United States have “the same interest in getting the Government’s work done.” *Boyle v. United Techs. Corp.*, 487 U.S. 500, 505 (1988). But the United States does not necessarily share an interest with the agents of a foreign sovereign, and those interests will routinely diverge, as they do in this case.

The rationale behind foreign immunity is different. It is based on the concept of comity between foreign sovereigns. And as *Samantar* makes clear, the decision of whether to extend immunity to a particular sovereign, as an act of comity, was historically a job for the Executive Branch, not the Judicial Branch. *See Samantar*, 560 U.S. at 311. That is why *Samantar* instructed that courts base their immunity determinations on the “established policy of the State Department.” *Samantar*, 560 U.S. at 312. Given that *Butters* pre-dated *Samantar*, the Fourth Circuit did not consider the State Department’s policy before deciding to extend the doctrine of domestic derivative immunity to foreign agents. But in *Yousuf*, on remand from *Samantar*, the Fourth Circuit gave “substantial weight” to the State Department’s contrary and considered views that a U.S. citizen normally should *not* be afforded such immunity. 699 F.3d at 777. For these reasons, the Court declines to apply *Butters* and extend the doctrine of domestic sovereign immunity to foreign sovereigns. And for the same reasons, the Court rejects *Ivey v. Lynch*, which adopted *Butters*’s reasoning. *See* 2018 U.S. Dist. LEXIS 133656 at *20.

The *Alicog* decision likewise fails to help the defendants. With little explanation, *Alicog* granted immunity for two U.S. citizens simply because “they were agents of the Saudi

government” and Saudi Arabia was immune in the case. 860 F. Supp. at 384. But as explained above, that conclusion is inconsistent with the State Department’s policy. And *Alicog* did not purport to apply the common law of foreign-official immunity at all. The Southern District of Texas stated instead that its decision as to the American defendants’ immunity was made “[u]nder Texas law,” *id.* at 381, not the federal common law of foreign-official immunity. This may explain why the court never examined the policies of the State Department or the principles of conduct-based immunity in reaching its conclusion.

Finally, in their briefs, neither party has cited to *Rishikof*, a case from this District in which the court afforded immunity to a U.S. citizen after a car accident that happened while he was delivering a package for the Swiss Confederation. 70 F. Supp. 3d at 10. Nonetheless, the Court declines to reach the same conclusion. First, the issue of whether foreign-official immunity extends to ordinary U.S. citizens was not at issue nor briefed by the parties prior to that decision; rather, *Rishikof* merely sought to determine whether an agent—as opposed to a formal official—could qualify for immunity under the common law. *See id.* at 12–13. Second, the court neglected to consider the established policies of the State Department in arriving at its conclusion. *See id.* And third, the defendant in *Rishikof* was both formally “an employee of Switzerland,” and the Swiss Confederation had “agreed to accept any legal liability for [his] actions that ar[ose] out of the claims.” *Id.* at 10. None of these circumstances are present here.

In sum, the Court concludes that the State Department would not grant immunity to these defendants, and no case that the defendants have identified affects that conclusion. Thus, assuming the State Department test is the proper test at step two, the defendants do not “satisfy the requisites for conduct-based immunity.” *Lewis*, 918 F.3d at 146. The Court will deny the defendants’ Rule 12(b)(1) motion to dismiss on this independent ground.

2. *Restatement Test*

The defendants also fail to satisfy the Restatement test because they “have not satisfied the necessary third element of conduct-based immunity” of Restatement § 66(f). *Lewis*, 918 F.3d at 147. This element requires courts to ask whether “exercising jurisdiction would serve to enforce a rule of law against the foreign state.” *Id.* at 146. It “would allow for immunity when a judgment against the official would bind (or be enforceable against) the foreign state.” *Id.*

This case falls squarely under *Lewis*. Like the defendants in *Lewis*, the defendants here have offered nothing “to show that [Broidy] seeks to draw on the [Qatari] treasury or force the state to take specific action, as would be the case if the judgment were enforceable against the state.” *Id.* at 147. To the contrary, and just as in *Lewis*, Broidy is suing the defendants “in their individual capacities” and “is not seeking compensation out of state funds.” *Id.* Thus, “[i]n cases like this one, in which the plaintiff pursues an individual-capacity claim seeking relief against an official”—or, by the same logic, an agent—“in a personal capacity, exercising jurisdiction does not enforce a rule against the foreign state.” *Id.*

The defendants respond that “Qatar is truly the party in interest” because allowing this case to proceed would require Qatar “to monitor, participate in, and object to discovery” to protect Qatar’s “sensitive, foreign-policy related information” from discovery. Defs.’ First Reply at 23, Dkt. 44. They also argue that “exercising jurisdiction here will necessarily affect Qatar’s decisions with respect to the hiring of contracts and agents to advance its interest in the United States.” *Id.* But the defendants in *Lewis* made similar arguments, and yet the court concluded that “these collateral effects “are too attenuated to be equated with the direct fiscal impacts on the foreign state that are contemplated by the restatement.” *Lewis*, 918 F.3d at 147. So too here. Vague assertions about what Qatar might do during discovery and amorphous

predictions about how this case might affect Qatar’s future decisions simply do not establish “direct fiscal impacts on the foreign state.” *Id.*

The Court concludes that the defendants “have not satisfied the necessary third element of conduct-based immunity” under the Restatement and need not address the first two elements. *Id.* Thus, assuming Restatement § 66(f) supplies the proper test at step two, the defendants do not “satisfy the requisites for conduct-based immunity.” *Id.* at 146. The Court will deny the defendants’ Rule 12(b)(1) motion to dismiss on this independent ground.

B. Counts I and II: RICO Claims

The RICO statute makes it “unlawful for any person employed by or associated with any enterprise engaged in, or the activities of which effect, interstate or foreign commerce, to conduct or participate, directly or indirectly, in the conduct of such enterprise’s affairs through a pattern of racketeering activity” 18 U.S.C. § 1962(c). This crime has four elements: “(1) conduct (2) of an enterprise (3) through a pattern (4) of racketeering activity.” *Sedima, S.P.R.L. v. Imrex Co.*, 473 U.S. 479, 496 (1985). A person who violates this section also faces civil liability because “[a]ny person injured in his business or property by reason of a violation of section 1962” may sue in federal district court and recover treble damages, costs, and attorney’s fees. *Id.* § 1964(c).

There are several requirements for proving a pattern of racketeering activity. First, the plaintiff must show “the commission of at least two predicate racketeering offenses over a ten year period.” *W. Assocs. Ltd. P’ship, ex rel. Ave. Assocs. Ltd. P’ship v. Mkt. Square Assocs.*, 235 F.3d 629, 633 (D.C. Cir. 2001) (citing 18 U.S.C. § 1961(5)). In a multiple-defendant RICO scheme, “each defendant” must have committed two predicate offenses. *United States v. Philip Morris USA, Inc.*, 566 F.3d 1095, 1117 (D.C. Cir. 2009). Second, a plaintiff must show

relatedness—*i.e.*, that these “racketeering predicates . . . share similar purposes, results, victims, or methods of commission, or otherwise are interrelated by distinguishing characteristics.” *W. Assocs.*, 235 F.3d at 633 (quoting *H.J. Inc. v. Nw. Bell Tel. Co.*, 492 U.S. 229, 40 (1989)). And third, a plaintiff must show continuity—*i.e.*, that these racketeering predicates “amount to or pose a threat of continued activity.” *Id.* (quoting *H.J. Inc.*, 492 U.S. at 240). To do so, a plaintiff can show either “a threat of future criminal activity” (an open-ended scheme) or a “closed period of repeated conduct.” (a closed-ended scheme). *Id.* at 633.

Broidy has failed to plead a pattern of racketeering activity because he has not pled either an open- or a closed-ended scheme.

1. Open-Ended Scheme

To plead an open-ended scheme, a complaint must plausibly allege a “distinct” threat of further long-term racketeering activity or a “showing that the predicate acts or offenses are part of an ongoing entity’s regular way of doing business.” *H.J. Inc.*, 492 U.S. at 242. This threat must be “far more than a hypothetical possibility of further predicate acts.” *Pyramid Secur., Ltd. v. IB Resolution, Inc.*, 924 F.2d 1114, 1119 (D.C. Cir. 1991). But the Complaint here alleges “nothing suggesting any reason to expect that these defendants, together or separately, will again engage in RICO-violating conduct.” *Edmondson & Gallagher v. Alban Towers Tenants Ass’n*, 48 F.3d 1260, 1264 (D.C. Cir. 1995). The alleged hacking already has happened, and the stories that were meant to silence Broidy already have been published. A “one time racket” like this one is not an open-ended scheme. *Hughes v. Consol-Pa. Coal Co.*, 945 F.2d 594, 610–11 (3d Cir. 1991).

The Complaint tries to create open-ended continuity by alleging that “[m]edia organizations are still relying on information stolen from Mr. Broidy’s computer systems and email servers to publish stories to damage his image.” Complaint ¶ 255. But though this ongoing

activity may suggest the possibility of future damages, it does not establish a distinct threat of ongoing or future racketeering activity by the defendants. As the Seventh Circuit correctly said:

When a thief steals \$100, the law does not hold him to a new theft each time he spends one of those dollars. The same is true of [stolen proprietary information] [The] subsequent and varied uses of the stolen [information] would not constitute new offenses but would go only to the issue of damages.

Mgmt. Comput. Servs. v. Hawkins, Ash, Baptie & Co., 883 F.2d 48, 51 (7th Cir. 1989). Thus, [e]ven if a future post repeats the same information, it will still not be in a furtherance of the sole scheme alleged.” *Ctr. for Immigration Studies v. Cohen*, 410 F. Supp. 3d 183, 193 (D.D.C. 2019) (declining to find open-ended continuity when defendants tried to “falsely designate [the plaintiff as] a hate group and destroy it” through blog entries).

Broidy argues that “the threat of release of stolen documents, including trade secrets and copyrighted materials, continues to this day.” Broidy’s Opp’n to Mot. to Dismiss at 76. The problem is, this allegation does not appear in the Complaint. The Complaint does allege that the scheme “began in December 2017 and is ongoing,” but it provides no specific allegations to support this claim beyond a May 21, 2018 news article related to the allegedly hacked materials. Complaint ¶ 137. At most, this allegation suggests a scheme that lasted for about five months, not an ongoing scheme that continues to this day. In addition, even if the Complaint had alleged an ongoing threat of releasing the stolen materials, that ongoing threat would be to further the same goal, not an open-ended scheme of racketeering activity. *See Roe v. Bernabei & Wachtel PLLC*, 85 F. Supp. 3d 89, 101 (D.D.C. 2015) (finding no pattern of racketeering activity despite possibility that the defendants would continue to use stolen intellectual property). Nor would a vague, unspecified “threat of release of stolen documents,” Broidy’s Opp’n to Mot. to Dismiss at 76, establish the “distinct” threat required for establishing an open-ended scheme. *H.J. Inc.*, 492 U.S. at 242. For all these reasons, Broidy has failed to plead an open-ended scheme.

2. *Closed-Ended Scheme*

Broidy has not adequately pled a closed-ended scheme either. Courts consider six factors to determine whether a plaintiff has established a closed-ended scheme: “the number of unlawful acts, the length of time over which the acts were committed, the similarity of the acts, the number of victims, the number of perpetrators, and the character of the unlawful activity.” *W. Assocs.*, 235 F.3d at 633 (internal quotation marks omitted). This standard “presents a flexible guide for analyzing RICO allegations.” *Id.* at 634. Even so, a few baseline requirements apply. A plaintiff must allege that the predicate acts were “committed over a period longer than a few weeks or months.” *Id.* at 636 (internal quotation marks omitted); *see also H.J. Inc.*, 492 U.S. at 242 (“Congress was concerned in RICO with long-term criminal conduct.”). And it is “‘virtually impossible for plaintiffs to state a RICO claim’” if they allege “only a single scheme, a single injury, and few victims.” *W. Assocs.*, 235 F.3d at 634 (quoting *Edmondson*, 48 F.3d at 1263).

The alleged scheme here fails even to meet these baseline requirements. To start, “the time involved here is too short” because Broidy alleges “actions that took place over a mere five months.” *Bridges v. Lezell Law, PC*, 842 F. Supp. 2d 261, 266 (D.D.C. 2012); *see also Ganzi v. Wash.-Baltimore Reg’l 2012 Coal.*, 98 F. Supp. 2d 54, 58 (D.D.C. 2000) (holding that eight months was too short). The unidentified hackers allegedly first targeted Broidy on December 27, 2017, Complaint ¶ 87, and the last allegation involving any of the defendants was Howard’s post-publication call with a reporter on May 22, 2018, Complaint ¶ 133.

In addition, Broidy alleges only a single scheme to “retaliate against, discredit, and ultimately silence Mr. Broidy” by “manufacturing negative news stories [and] exposing his confidential communications and trade secrets to the public.” Complaint ¶¶ 2, 8. This is not enough to support a pattern of racketeering activity. *See Ambellu v. Re’ese Adbarat Debre Selam Kidist Mariam*, 406 F. Supp. 3d 72, 82 (D.D.C. 2019) (declining to find a pattern from a

single scheme resulting in a single injury even though it “affected many victims”).

Finally, this scheme has at most a “few victims”—Broidy, his spouse, his executive assistant, and possibly Mowbray—not enough victims to create a closed-ended racketeering scheme. *Edmondson*, 48 F.3d at 1265; *see* Complaint ¶¶ 90, 95–96, 106. The Complaint alludes to other victims, alleging that the Qatari Enterprise committed wire fraud by targeting “more than 1,400 email addresses.” Complaint ¶¶ 9, 108–09, 213, 254. But this allegation about these other “predicate acts of mail and wire fraud necessary to sustain a RICO claim are not pled with nearly the specificity required by the heightened pleading standard of Rule 9(b).” *Bates v. Nw. Human Servs.*, 466 F. Supp. 2d 69, 88 (D.D.C. 2006). When the alleged predicate acts are wire fraud, “courts have been particularly sensitive to Rule 9(b)’s pleading requirements in RICO cases . . . and have further required specific allegations as to which defendant caused what to be mailed and when and how each mailing furthered the fraudulent scheme.” *Id.* at 89. The allegation must “state the time, [the] place and content of the false misrepresentation, the fact misrepresented[,] and what was retained or given up as a consequence of the fraud.” *Id.* This allegation is not nearly specific enough to satisfy Rule 9(b)—it does not specify the consequence of the fraud or the time, place, or the content of the misrepresentation.

In sum, the alleged scheme had a single goal, targeted only a few victims, and took just five months from start to finish. Such activities do not form a closed-ended pattern of racketeering activity. *See W. Assocs.*, 235 F.3d at 635 (holding that “dozens of predicate acts extending continually over an eight-year period” was insufficient where there was a single scheme, single injury, and single set of partnership victims); *Edmondson*, 48 F.3d at 1265 (holding that thirteen predicate acts committed over three years was “not enough to overwhelm” the single scheme, single injury, and few victims factors).

By not adequately pleading continuity, Broidy has not adequately pled a pattern of racketeering activity. The Court will therefore dismiss Count I, which alleges a substantive civil RICO violation. The Court also will dismiss Count II, which alleges a RICO conspiracy, because an agreement to commit acts that do not form a pattern of racketeering activity is not an unlawful agreement under the RICO statute.

C. Other Federal Statutory Claims

1. Count III: Stored Communications Act

The Stored Communications Act provides a private cause of action against a defendant who “intentionally accesses without authorization a facility through which an electronic communication service is provided.” 18 U.S.C. §§ 2701(a)(1), 2707(a). Broidy does not allege that any of the defendants themselves accessed BCM’s computer systems; rather, he alleges that the defendants “conspired” with others who did. Complaint ¶ 270.

Every court to decide whether the Stored Communications Act permits private actions under secondary liability theories like Broidy’s has held that it does not. *See, e.g., Council on Am.-Islamic Rels. Action Network, Inc. v. Gaubatz*, 891 F. Supp. 2d 13, 27 (D.D.C. 2012); *Freeman v. DirecTV, Inc.*, 457 F.3d 1001, 1009 (9th Cir. 2006); *Vista Mktg., LLC v. Park*, 999 F. Supp. 2d 1294, 1296 (M.D. Fla. 2014); *Jones v. Glob. Info. Grp., Inc.*, Civil Action No. 3:06-00246-JDM, 2009 U.S. Dist. LEXIS 23887, at *9 (W.D. Ky. Mar. 25, 2009).² The Court agrees.

The Stored Communications Act’s “plain language shows that Congress had one category of offenders in mind—*i.e.*, those who directly access, or exceed their authority to

² Though Broidy argues that one court has applied the Stored Communication Act to permit secondary liability, *see Tyan, Inc. v. Garcia*, No. CV1505443MWFJPRX, 2017 WL 1658811, at *14 (C.D. Cal. May 2, 2017), in that case, the sole defendant “personally hijacked” the plaintiff’s website, *id.* at *9.

access, a facility through which an electronic communication service is provided.” *Gaubatz*, 891 F. Supp. 2d at 26. In drawing the boundaries of civil liability under the Stored Communications Act, “Congress made no mention of conspiracy, aiding and abetting, or any other form of secondary liability.” *Id.* at 27. And “when Congress enacts a statute under which a person may sue and recover damages from a private defendant for the defendant’s violation of some statutory norm, there is no general presumption that the plaintiff may also sue aiders and abettors.” *Cent. Bank, N.A. v. First Interstate Bank, N.A.*, 511 U.S. 164, 182 (1994). The same principle applies to bar recovery from coconspirators, *see, e.g., Gaubatz*, 891 F. Supp. 2d at 27; *Dinsmore v. Squadron, Ellenoff, Plesent, Sheinfeld & Sorkin*, 135 F.3d 837, 842 (2d Cir. 1998), because Congress knows how to provide private plaintiffs with an action for secondary liability when it sees fit, *see, e.g.,* 18 U.S.C. §§ 1030(a)(2), 1962(d).

The plaintiffs urge that the Stored Communications Act’s legislative history and the policies underlying the Act are enough to overcome the presumption “that ‘statutory silence on the subject of secondary liability means there is none.’” *Owens v. BNP Paribas, S.A.*, 235 F. Supp. 3d 85, 93 (D.D.C. 2017) (quoting *Boim v. Holy Land Found. for Relief & Dev.*, 549 F.3d 685, 689 (7th Cir. 2008) (en banc)). But “[p]olicy considerations cannot override [the Court’s] interpretation of the text and structure of the [Stored Communications Act], except to the extent that they may help to show that adherence to the text and structure would lead to a result so bizarre that Congress could not have intended it.” *Cent. Bank*, 511 U.S. at 188 (internal quotation marks omitted). And interpreting the Stored Communications Act to lack secondary liability is not a “bizarre” result. *Id.* The Court will thus dismiss Count III alleging violations of the Stored Communications Act.

2. *Count IV: Computer Fraud and Abuse Act*

The Computer Fraud and Abuse Act penalizes one who “intentionally accesses a

computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer.” 18 U.S.C. § 1030(a)(2). A “protected computer” includes one that “is used in or affect[s] interstate or foreign commerce or communication.” *Id.* § 1030(e)(2). Unlike the Stored Communications Act, the Computer Fraud and Abuse Act extends liability to “[w]hoever conspires to commit” an offense under the Act. *Id.* § 1030(b). “Any person who suffers damage or loss by reason of a violation of [the Computer Fraud and Abuse Act] may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.” *Id.* § 1030(g). Further, a civil plaintiff alleging damages must plead only that the aggregate value of the loss be in excess of \$5,000, *see id.* § 1030(c)(4)(a)(1)(I), which Broidy has done, *see* Complaint ¶ 286.

Because the Computer Fraud and Abuse Act supports secondary liability, Broidy has plausibly stated a claim. The Complaint states in detailed factual allegations the hacking scheme purportedly perpetuated by GRA and other members of the Qatari Enterprise to infiltrate the BCM servers. *See id.* ¶¶ 78–110. At the same time, the Complaint plausibly suggests that defendants were knowingly involved in the alleged conspiracy, as explained in the Court’s discussion of civil conspiracy (Count XIII) below. The Court will deny defendants’ motion to dismiss Count IV alleging violations of the Computer Fraud and Abuse Act.

3. *Count V: Defend Trade Secrets Act*

The Defend Trade Secrets Act permits plaintiffs to bring a private cause of action if they “own[] a trade secret that is misappropriated.” 18 U.S.C. § 1836(b)(1). A “trade secret” includes “all forms and types” of information that “derives independent economic value . . . from not being generally known” and for which “the owner . . . has taken reasonable measures to keep such information secret.” *Id.* § 1839(3). The term “misappropriation” includes the unauthorized “acquisition” or “disclosure or use of a trade secret of another” by one who, “at the time of

disclosure or use, knew or had reason to know that the knowledge of the trade secret was derived from or through a person who had used improper means to acquire the trade secret.” *Id.* § 1839(5). The Defend Trade Secrets Act further defines “improper means” to “include[] theft . . . or espionage through electronic or other means.” *Id.* § 1839(6). Broidy has plausibly alleged a Defend Trade Secrets Act violation.

First, the Complaint adequately pleads that a trade secret existed. To survive a motion to dismiss, Broidy “need not plead with specificity what particular proprietary information was misappropriated.” *DocMagic, Inc. v. Ellie Mae, Inc.*, 745 F. Supp. 2d 1119, 1145 (N.D. Cal. 2010). The Complaint states that “[t]he BCM server stored trade secrets including but not limited to highly confidential business plans and proposals, research supporting those plans and proposals including costs and service projections, information concerning business strategies and opportunities, and contacts for important business relationships.” Complaint ¶ 295. “Plaintiffs’ allegations permit [defendants] and the court ‘to ascertain at least the boundaries within which the secret[s] lie[],’ which is sufficient at the pleading stage.” *Willert v. Andre*, No. 17-cv-496-jdp, 2017 U.S. Dist. LEXIS 179770, at *11 (W.D. Wis. Oct. 31, 2017) (quoting *ECT Int’l, Inc. v. Zwerlein*, 597 N.W.2d 479, 482 (Ct. App. 1999)); *see also, e.g., Zeetogroup, LLC v. Fiorentino*, No. 19-CV-458 JLS (NLS), 2019 U.S. Dist. LEXIS 80648, at *7–*10 (S.D. Cal. May 13, 2019) (denying motion to dismiss Complaint alleging the misappropriation of customer lists and performance metrics associated with those lists). Broidy also plausibly has shown that his business plans, proposals, and research derive value from not being generally known in the investment management industry. *See* Complaint ¶¶ 11, 232, 234–35. And Broidy has likewise shown that he has taken reasonable measures to keep such information secret, such as maintaining the information “on secured servers that are protected by passwords, firewalls, and

antivirus software.” Complaint ¶ 233.

Second, the Complaint sufficiently pleads that defendants misappropriated the alleged trade secrets contained on the BCM server. The Complaint explains that each defendant received and possessed this proprietary information knowing that it was stolen from the server. *See* Complaint ¶¶ 116–17, 140, 159, 187, 300–02. And it charges the defendants with unlawfully disclosing that information to one another and the media prior to any publication. *See id.* ¶¶ 111–16, 138–59, 301. Indeed, Howard first had conversations with reporters just two days after the hack infiltrated BCM’s servers, *id.* ¶ 119, and Muzin and Allaham spoke about “[getting] the press going after Broidy” just a week later, *id.* ¶ 140. Thus, Broidy has plausibly alleged a violation of Defend Trade Secrets Act by each of the defendants.

The defendants argue that the Court cannot award damages as well as grant an injunction to prevent further misuse here because “the [Complaint] impermissibly invokes the *criminal* provisions [of the Defend Trade Secrets Act].” Howard’s Mot. to Dismiss at 42. It is true that damages would be unavailable if the Complaint alleged secondary liability only, as provided for under the criminal provisions of the Act. *See Steves & Sons, Inc. v. Jeld-Wen, Inc.*, 271 F. Supp. 3d 835, 842–43 (E.D. Va. 2017). But the Complaint alleges primary liability. It states that the defendants *themselves* “improperly disclosed and misappropriated Plaintiffs’ trade secrets without consent or authorization when they widely disseminated those trade secrets to fellow members of the Qatari Enterprise and to media organizations for publication.” Complaint ¶ 301; *see also* 18 U.S.C. § 1839(5) (stating that a defendant can misappropriate a trade secret so long as he “knew or had reason to know that the knowledge of the trade secret was derived from or through a person who had used improper means to acquire [it]”).

To the extent that the Complaint alleges secondary liability as well, that theory of liability

is unavailable for a civil action. *See Steves & Sons*, 271 F. Supp. 3d at 842–43; *Genentech, Inc. v. JHL Biotech, Inc.*, No. C 18-06582 WHA, 2019 U.S. Dist. LEXIS 36140, at *35 (N.D. Cal. Mar. 1, 2019) (“Genentech cites no authority suggesting that Section 1836(b) of the Defend Trade Secrets Act provides for a stand-alone private action for conspiracy to misappropriate trade secrets. . . .”). The Court will not permit the plaintiffs to advance this theory going forward, and they must prove that each defendant individually misappropriated at least one trade secret. With that caveat, the Court will deny the defendants’ motion to dismiss Count V alleging violations of the Defend Trade Secrets Act.

D. State Statutory Claims

1. Count VI: California Uniform Trade Secrets Act

Like its federal counterpart, the California Uniform Trade Secrets Act recognizes a private cause of action for damages and injunctive relief following the misappropriation of a plaintiff’s trade secrets. *See* Cal. Civ. Code §§ 3426.2; 3426.3. The California Uniform Trade Secrets Act “offer[s] essentially the same definitions” for “trade secret” and “misappropriation” as the Defend Trade Secrets Act. *Waymo LLC v. Uber Techs., Inc.*, No. C 17-00939 WHA, 2017 U.S. Dist. LEXIS 73843, at *22 (N.D. Cal. May 11, 2017); *see* Cal. Civ. Code § 3426.1. “A cause of action for monetary relief under California Uniform Trade Secrets Act . . . consist[s] of the following elements: (1) possession by the plaintiff of a trade secret; (2) the defendant’s misappropriation of the trade secret, meaning its wrongful acquisition, disclosure, or use; and (3) resulting or threatened injury to the plaintiff.” *Silvaco Data Sys. v. Intel Corp.*, 109 Cal. Rptr. 3d 27 (Ct. App. 2010).

For the reasons stated above regarding alleged violations of the Defend Trade Secrets Act, Broidy has plausibly established each of these elements. The Court will therefore deny defendants’ motion to dismiss Count VI.

The defendants argue that the California Uniform Trade Secrets Act preempts most of Broidy's other claims arising under California law. *See* Howard's Mot. to Dismiss at 44, 49, 51, 54. The Act specifically provides that it "does not affect . . . civil remedies that are not based upon misappropriation of a trade secret." Cal. Civ. Code § 3426.7(b). But even so, this provision has been read to "implicitly preempt[] alternative civil remedies [that are] based on trade secret misappropriation." *K.C. Multimedia, Inc. v. Bank of Am. Tech. & Operations, Inc.*, 90 Cal. Rptr. 3d 247, 258 (Ct. App. 2009). This "determination of whether a claim is based on trade secret misappropriation is largely factual." *Id.* "At the pleadings stage, the supersession analysis asks whether, stripped of facts supporting trade secret misappropriation, the remaining factual allegations can be reassembled to independently support other causes of action." *Waymo, LLC v. Uber Techs., Inc.*, 256 F. Supp. 3d 1059, 1062 (N.D. Cal. 2017); *see Silvaco*, 109 Cal. Rptr. 3d at 51.

The Court concludes that they can. As set forth in the Complaint, Broidy's remaining state-law claims alleging receipt and possession of stolen property, public disclosure of private facts, intrusion upon seclusion, and conversion "each have a basis independent of any misappropriation of a trade secret." *Angelica Textile Servs., Inc. v. Park*, 163 Cal. Rptr. 3d 192, 202 (Ct. App. 2013). This is because those claims "do[] not require that the confidential information qualify as a 'trade secret'" in order for Broidy to prevail. *Integral Dev. Corp. v. Tolat*, 675 F. App'x 700, 704 (9th Cir. 2017); *see, e.g., Javo Bev. Co. v. Cal. Extraction Ventures, Inc.*, No. 19-CV-1859-CAB-WVG, 2019 U.S. Dist. LEXIS 207483, at *15 (S.D. Cal. Dec. 2, 2019); *Leatt Corp. v. Innovative Safety Tech., Ltd. Liab. Co.*, No. 09-CV-1301 - IEG (POR), 2010 U.S. Dist. LEXIS 71362, at *20 n.5 (S.D. Cal. July 15, 2010). It is quite plausible—likely even—that many of the emails that the defendants allegedly misused would not

constitute nor contain a trade secret. *See* Complaint ¶¶ 111–59; *see also id.* ¶ 325 (describing the emails as containing “private communications, documents, trade secrets and intellectual property”—not just trade secrets alone). “At this point in the case, the status of the information is merely a matter of allegation and until the distinction is made between [Broidy]’s allegedly misappropriated trade secret information and its confidential or non-confidential proprietary non-trade secret information, the question of preemption should not be addressed.” *Amron Int’l Diving Supply, Inc. v. Hydrolinx Diving Commun., Inc.*, No. 11-CV-1890-H (JMA), 2011 U.S. Dist. LEXIS 122420, at *30 (S.D. Cal. Oct. 21, 2011). The Court concludes that the California Uniform Trade Secrets Act does not preempt Broidy’s remaining state-law claims.

2. *Count VII: Receiving Stolen Property*

i. Choice of Law

The parties dispute whether California or District of Columbia law should govern Broidy’s claim of receipt and possession of stolen property. In determining which law applies, the Court uses the District of Columbia’s choice-of-law rules. *See Klaxon Co. v. Stentor Elec. Mfg. Co.*, 313 U.S. 487, 496 (1941); *Wu v. Stomber*, 750 F.3d 944, 949 (D.C. Cir. 2014). The District of Columbia employs a “governmental interests” analysis in resolving choice-of-law issues. *District of Columbia v. Coleman*, 667 A.2d 811, 816 (D.C. 1995). When a “true conflict” exists between the laws of multiple jurisdictions, a court employing this analysis must “evaluate the governmental policies underlying the applicable laws and determine which jurisdiction’s policy would be more advanced by the application of its law to the facts of the case under review.” *Id.* (citing *Hercules & Co. v. Shama Restaurant*, 566 A.2d 31, 40–41 (D.C. 1989)). “Part of the test of determining the jurisdiction whose policy would be most advanced is determining which jurisdiction has the most significant relationship to the dispute.” *Id.* In making this determination, the D.C. courts look to these four factors:

- a) the place where the injury occurred;
- b) the place where the conduct causing the injury occurred;
- c) the domicile, residence, nationality, place of incorporation and place of business of the parties; and
- d) the place where the relationship is centered.

Id. When a plaintiff resides in a state with a plaintiff-protecting law, this test “typically leads to the application of the law of plaintiff’s domicile, as the state with the greatest interest in providing redress to its citizens.” *Beer v. Islamic Republic of Iran*, 574 F. Supp. 2d 1, 10 (D.D.C. 2008).

A true conflict exists here. The California legislature has specifically provided for a private cause of action for victims of the receipt and possession of stolen property, *see* Cal. Pen. Code § 496, while the D.C. Council has not, *see* D.C. Code § 22-3232. Though it is unclear whether the D.C. Council acted deliberately in omitting this civil cause of action from the statutory scheme, a “failure to provide a statutory cause of action does not necessarily demonstrate that [D.C.] has no underlying interest at stake,” *Levine v. Am. Psychological Ass’n*, 766 F.3d 39, 52 (D.C. Cir. 2014).

California’s policy would be more advanced by the application of its law here. In providing for a private cause of action, the California “Legislature believed the deterrent effect of criminal sanctions was not enough to reduce thefts.” *Bell v. Feibush*, 151 Cal. Rptr. 3d 546, 551 (Ct. App. 2013). “The means to reduce thefts, the Legislature concluded, was to dry up the market for stolen goods by permitting treble damage recovery” for victims without the state having to first “decide[] to initiate and complete prosecutions.” *Id.* It would seriously undermine California’s strong interests in deterring crime and compensating plaintiffs not to recognize a cause of action for California plaintiffs harmed and feeling injury in California by the theft of property stored on their California servers. *See FMC Corp. v. Capital Cities/ABC*,

Inc., 915 F.2d 300, 302 (7th Cir. 1990) (“[T]he fact that [plaintiff] is located in California and is feeling the loss of its documents there means that the ‘most significant contacts’ . . . are to be found in California.”).

By contrast, the District of Columbia’s interests are only weakly implicated in this case. The District has no real interest in shielding these non-resident individual defendants from a civil suit alleging the commission of a crime directed at the California property of a California resident. And it certainly does not want to countenance non-residents who have entered the District for the commission of a crime under District law. *See* D.C. Code § 22-3232. In addition, the District’s courts have recognized a similar civil cause of action for “any unlawful exercise of ownership, dominion or control over the personal property of another in denial or repudiation of his rights thereto.” *Duggan v. Keto*, 554 A.2d 1126, 1137 (D.C. 1989) (internal quotation marks omitted). It thus does not represent a significant departure from District of Columbia policy to recognize this cause of action for receipt and possession of stolen property. The Court will apply California law.

ii. Merits

California law makes it unlawful for any person to “receive[] any property that has been stolen or that has been obtained in any manner constituting theft or extortion, knowing the property to be so stolen or obtained.” Cal. Pen. Code § 496(a). “Any person who has been injured by a violation of [this law] may bring an action for three times the amount of actual damages, if any, sustained by the plaintiff, costs of suit, and reasonable attorney’s fees.” *Id.* § 496(c). At the pleadings stage, a civil plaintiff must plausibly allege “three elements: (a) the property was stolen, and (b) the defendant was in possession of it, (c) knowing it was stolen.” *Verdugo-Gonzalez v. Holder*, 581 F.3d 1059, 1061 (9th Cir. 2009); *see also Switzer v. Wood*, 247 Cal. Rptr. 3d 114, 121 (Ct. App. 2019).

The Complaint establishes each of these three elements. First, the electronic information and documents were stolen from Broidy by the alleged cyberattack. Complaint ¶¶ 97–110. This electronically stored information qualifies as Broidy’s “property” under California law. Indeed, “[a]nything that can be the subject of theft can also be property under section 496.” *People v. Gopal*, 217 Cal. Rptr. 487, 497 (Ct. App. 1985). For example, in *Am. Shooting Ctr., Inc. v. Secfor Int’l*, No. 13cv1847 BTM(JMA), 2016 U.S. Dist. LEXIS 40523, (S.D. Cal. Mar. 28, 2016), the court faced the issue of whether defendants could be held liable under the California provision at issue here for their theft of training materials taken from the plaintiff’s computers. *See id.* at *5, *25. In denying the defendants’ motion to dismiss, the court held that “documents on the computers may . . . be deemed property subject to theft under the statute.” *Id.* at *26; *see also Kremen v. Cohen*, 337 F.3d 1024, 1029–30 (9th Cir. 2003) (holding that a “domain name” fell within the “broad concept” of property which “includes every intangible benefit and prerogative susceptible of possession or disposition”). Similarly, the intangible electronic information contained on Broidy’s servers constitutes property which is capable of being stolen.

At the same time, the Complaint plausibly alleges that the defendants were in possession of this stolen information. *See* Complaint ¶¶ 115–17, 140–41, 159, 170. And it plausibly suggests that the defendants knew that the information was stolen, given their ties to the alleged Qatari Enterprise, the close proximity of their communications to the date of the hacking, and the fact that Allaham and Muzin communicated regarding Benomar’s trip to Qatar to retrieve the emails. *See id.* ¶¶ 111–12, 115–22, 140–41, 187. The Court will deny defendants’ motion to dismiss Count VII.

3. *Count XIII: California Comprehensive Computer Data Access and Fraud Act*

The California Comprehensive Computer Data Access and Fraud Act penalizes any

person who “[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network.” Cal. Pen. Code § 502(c)(2). It also provides a private cause of action for those harmed by violations of the Act. *Id.* § 502(e)(1). But just like the Stored Communications Act, it does not provide for secondary liability in a civil action. “When a statute is precise about who can be liable courts should not implicitly read secondary liability into the statute.” *Freeman*, 457 F.3d at 1006; *Gaubatz*, 891 F. Supp. 2d at 27; *see Cent. Bank*, 511 U.S. at 182. Broidy’s California Comprehensive Computer Data Access and Fraud Act claim therefore fails because the Complaint does not allege that any of the defendants personally hacked or assisted in the hacking of BCM’s servers.³ *See Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 863 (N.D. Cal. 2011) (refusing “to impose liability on defendant for third party hackers’ unauthorized access”).

Broidy urges that the California Comprehensive Computer Data Access and Fraud Act extends liability to one who “provides or assists in providing a means of accessing a computer, computer system, or computer network.” Cal. Pen. Code § 502(c)(6). But that does not mean that any coconspirator inevitably violates the statute. To the contrary, to “provid[e] a means of accessing” a computer system, a defendant must facilitate the actual unauthorized access in some way.” *See Claridge*, 785 F. Supp. 2d at 863 (noting that the California Comprehensive Computer Data Access and Fraud Act does not extend to those “who took no active role in tampering with, or in gaining unauthorized access to computer systems”). That is, a defendant must “make, procure, or furnish for *future* use” the method of accessing a computer system, or otherwise “supply,” “afford,” or “contribute” the means by which the system is accessed.

³ Because Broidy’s claim fails under California law, the Court need not address the defendant’s argument that D.C. law, which does not recognize a private cause of action similar to that in the California Comprehensive Computer Data Access and Fraud Act, should apply instead.

Provide, Black’s Law Dictionary 1224 (6th ed. 1990) (emphasis added); *see also Means*, Black’s Law Dictionary 980 (“That through which, or by the help of which, an end is attained[.]”). The Complaint does not allege that defendants did any such thing, alleging only that they received the information after the cyberattack. *See, e.g.*, Complaint ¶¶ 281, 337; *see also* Broidy’s Opp’n to Mot. to Dismiss at 122 (“Of course, plaintiffs have been very straightforward in saying that they do not currently accuse the defendants of having participated in the [hacking].”). The Court will dismiss Count VIII.

E. State Common-Law Claims

1. Count IX: Public Disclosure of Private Facts

To state a claim for public disclosure of private facts under California law, a complaint must establish: “(1) public disclosure (2) of a private fact (3) which would be offensive and objectionable to the reasonable person and (4) which is not of legitimate public concern.” *Shulman v. Grp. W Prods., Inc.*, 955 P.2d 469, 478 (Cal. 1998) (internal quotation marks omitted).

Turning to the first element, an actionable disclosure of a private fact must be “widely published and not confined to a few persons or limited circumstances.” *Hill v. Nat’l Collegiate Athletic Ass’n*, 865 P.2d 633, 648 (Cal. 1994) (citing Restatement (Second) of Torts § 652D cmt. a (1977) (stating that the private fact must be communicated to the “public at large”)). Because of this limitation, Broidy can succeed on his claim only if he can show that the information that was actually published in the various news articles about him satisfies the other three elements of the tort. The private relaying of unpublished information to reporters does not amount to a “public disclosure,” regardless of whether it satisfies the other three elements.

Turning to the second element, Broidy does not allege specifically what he views as the “private facts” published in the five articles referenced in the Complaint, but at least some could

reasonably be viewed as private. The first article from the *New York Times* reveals parts of a memorandum that Broidy wrote regarding a private meeting he had with President Trump to influence foreign policy in the Middle East. *See* Dkt. 41-4, at 2. It states that Broidy pressed the President repeatedly to meet with the UAE’s crown prince, lobbied the President to fire Secretary of State Rex Tillerson, and spoke with the President “about politics and the fund-raising efforts for the midterm elections as well as the state of affairs at the [Republican National Committee].” *See id.* at 6–7. The second article from the Associated Press notes that George Nader, a UAE adviser and witness in the Mueller investigation, sent Broidy \$2.5 million which was allegedly “intended to fund Broidy’s Washington advocacy regarding Qatar.” Dkt. 41-5, at 4. The third article published by *McClatchy* reveals that Broidy attempted to use a Romanian visit by congressman Ed Royce to help Broidy’s defense firm “win points” with controversial political allies. Dkt 41-6, at 2. It alludes to documents suggesting that Broidy met with the U.S. ambassador to Romania, was in Romania around the time of Royce’s trip, tried to convince Royce not to meet with Romania’s top anti-corruption prosecutor, and sought the assistance of the chair of the House Foreign Affairs Committee to win a U.S. Commerce Department endorsement for his company in Romania. *Id.* at 3–4. *McClatchy* also alluded to a draft agreement through which Broidy would have paid a company connected to a “controversial Romanian businessman and a movie producer who played a key role in the New York state pension scandal” for business they helped him secure in Romania and surrounding countries. *Id.* at 5. The fourth article from the Associated Press adds that “in return for pushing anti-Qatar policies” to the White House, Broidy “expected huge consulting contracts from Saudi Arabia and the UAE,” potentially worth over a billion dollars. Dkt 41-7, at 2, 5. The fifth article from the *Huffington Post* details emails showing that Broidy’s wife tried “to scuttle a Justice Department

investigation into money laundering,” and that Broidy “tried to use his influence with the Trump administration to help.” Dkt. 41-8, at 2. At least some of these business dealings and personal memoranda could be considered private facts.

But regardless, the “nature of the fact[s] disclosed is not so ‘offensive and objectionable’ to meet the requirements of the third element.” *Daly v. Viacom, Inc.*, 238 F. Supp. 2d 1118, 1124–25 (N.D. Cal. 2002) (granting motion to dismiss). “It is only where the intrusion has gone beyond the limits of decency that liability accrues.” *Gill v. Hearst Pub. Co.*, 253 P.2d 441, 444 (1953). And the facts contained in the articles “are simply not offensive to the degree of morbidity or sensationalism.” *Virgil v. Sports Illustrated*, 424 F. Supp. 1286, 1289 (S.D. Cal. 1976); *see also Virgil v. Time, Inc.*, 527 F.2d 1122, 1129 n.11 (9th Cir. 1975) (endorsing these terms “as illustrative of the degree of offensiveness which should be present”). Indeed, the Court cannot find any case where publishing a private meeting with a politician or business associate—or revealing any business dealings for that matter—was “so offensive as to ‘shock the ordinary sense of decency or propriety.’” David A. Elder, *Privacy Torts* § 3:6 (2019) (quoting *Gill*, 253 P.2d at 445) (collecting cases).

Broidy’s contention that it is per se offensive to disclose facts that had been obtained by the cyberhacking of a third party is unpersuasive because it conflates public disclosure of private facts with the separate tort of intrusion upon seclusion. The third element of the former looks to the “nature” of the disclosed *facts* themselves, not to how those facts were obtained. *Daly*, 238 F. Supp. 2d at 1124. That is, “the *matter* made public must be one which would be *offensive* and objectionable to a reasonable [person] of ordinary sensibilities.” *Forsher v. Bugliosi*, 608 P.2d 716, 725 (Cal. 1980) (first emphasis added). Broidy’s claim thus fails on the third element.

In addition, Broidy's claim fails on the fourth element because the information contained in the articles is undoubtedly newsworthy. A "lack of newsworthiness is an element of the 'private facts' tort," and so newsworthiness is "a complete bar to common law liability." *Shulman*, 955 P.2d at 478. "Courts must decide whether a publication is newsworthy based upon: (1) the social value of the published facts; (2) the extent of the intrusion into ostensibly private matters, and (3) the extent to which a party voluntarily assumed a position of public notoriety." *Four Navy Seals & Jane Doe v. AP*, 413 F. Supp. 2d 1136, 1146 (S.D. Cal. 2005). "The newsworthiness inquiry focuses on the particular fact at issue that was disclosed, not on the general topic of the publication." *Doe v. Gangland Prods.*, 730 F.3d 946, 959 (9th Cir. 2013). The publication of private facts which "bear a logical relationship to the newsworthy subject . . . and are not intrusive in great disproportion to their relevance" cannot give rise to liability. *Schulman*, 955 P.2d at 478. "If there is room for differing views whether a publication would be newsworthy the question is one to be determined by the jury and not the court." *Times-Mirror Co. v. Superior Court*, 244 Cal. Rptr. 556, 562 (Ct. App. 1988). But this does not preclude a court from dismissing a public disclosure claim on newsworthiness grounds as a matter of law. See, e.g., *Four Navy Seals*, 413 F. Supp. 3d 1136; *Lorenzo v. United States*, 719 F. Supp. 2d 1208, 1215 (S.D. Cal. 2010); see also, e.g., *Shulman*, 955 P.2d at 488 (summary judgment).

All the articles here concern undeniably newsworthy subjects about a prominent businessman who has voluntarily assumed a position of public notoriety: meetings with the President to influence foreign affairs in the Middle East, funding anti-Qatari advocacy in Washington to secure lucrative consulting contracts with Saudi Arabia and the UAE, attempts to leverage a connection with the chair of the House Foreign Affairs Committee to win foreign

business contracts, and efforts to influence a billion-dollar Justice Department investigation. None of the facts contained in those articles lack a logical relationship to the newsworthy subject. Nor are they intrusive in a manner disproportionate to their relevance. Because the allegedly private facts were newsworthy, and for the independent reason that Broidy has failed to plead adequately that the revelation of any of them was offensive and objectionable to a reasonable person, the Court will dismiss Count IX.

2. *Count X: Intrusion Upon Seclusion*

The tort of intrusion upon seclusion “has two elements: (1) intrusion into a private place, conversation or matter, (2) in a manner highly offensive to a reasonable person.” *Shulman*, 955 P.2d at 490. For the first element, “the plaintiff must show the defendant penetrated some zone of physical or sensory privacy surrounding, or obtained unwanted access to data about, the plaintiff.” *Id.* The defendant may be held liable “only if the plaintiff had an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source.” *Id.* For the second element, “each case must be taken on its facts.” *Id.* at 494.

On a theory of primary liability, Broidy’s claim would fail because the Complaint does not allege that any of the defendants committed the intrusion. *See Nix v. Hoke*, 139 F. Supp. 2d 125, 133 & n.7 (D.D.C. 2001). But as explained below in the Court’s discussion of count XIII, Broidy has plausibly alleged that the defendants were part of a conspiracy. This allegation is sufficient to state a claim for intrusion upon seclusion. The Court agrees with decisions concluding that “hacking into a person’s private computer . . . would represent an intentional intrusion on the victim’s private affairs and that such an intrusion would be highly offensive to a reasonable person.” *Coal. for an Airline Passengers’ Bill of Rights v. Delta Airlines, Inc.*, 693 F. Supp. 2d 667, 675 (S.D. Tex. 2010); *see also Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1058

(N.D. Cal. 2014) (obtaining mobile address books). The Court will deny defendants’ motion to dismiss Count X.

3. *Count XI: Conversion*

“Conversion is the wrongful exercise of dominion over the property of another. The elements of a conversion claim are: (1) the plaintiff’s ownership or right to possession of the property; (2) the defendant’s conversion by a wrongful act or disposition of property rights; and (3) damages.” *Lee v. Hanley*, 354 P.3d 334, 344 (Cal. 2015) (internal quotation marks omitted); *see also Shea v. Fridley*, 123 A.2d 358, 361 (D.C. 1956) (similar).

Though the parties dispute whether California or D.C. law applies, Broidy’s conversion claim fails either way. D.C. law is clear that the “mere copying of electronic data does not constitute conversion.” *Council on Am.-Islamic Rels. Action Network, Inc. v. Gaubatz*, 793 F. Supp. 2d 311, 339 (D.D.C. 2011); *see Hedgeye Risk Mgmt., LLC v. Heldman*, 271 F. Supp. 3d 181, 196 (D.D.C. 2017). And the mere copying of electronic data is precisely what Broidy alleges. *See* Complaint ¶ 359. The Complaint “is devoid of any allegation that Defendants deleted, corrupted, or otherwise interfered with Plaintiffs’ control over their electronic data.” *Gaubatz*, 793 F. Supp. at 340.

Broidy likewise fails to establish a claim of conversion under California law. As in D.C., “[t]he possession of copies of documents—as opposed to the documents themselves—does not amount to an interference with the owner’s property sufficient to constitute conversion.” *FMC*, 915 F.2d at 303 (applying California law). This principle is no different in the case of electronic documents. When “the alleged converter has only a copy of the owner’s property and the owner still possesses the property itself, the owner is in no way being deprived of the use of his property. The only rub is that someone else is using it as well.” *Id.* at 303–04; *see In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1075 (N.D. Cal. 2012) (refusing to recognize

conversion claim for personal information stored on Apple devices); *cf. Kremen*, 337 F.3d at 1034–35 (allowing conversion claim where defendant gave away the plaintiff’s right to use a domain name).

Broidy relies heavily on *Thyroff v. Nationwide Mut. Ins. Co.*, 864 N.E.2d 1272 (N.Y. 2007), to argue that “electronic records that were stored on a computer and were indistinguishable from printed documents [are] subject to a claim of conversion.” *Id.* at 1278. There, the defendant physically “repossessed” a leased computer system “and denied Thyroff further access to the computers and all electronic records and data.” *Id.* at 1273. This exclusion was critical to the court’s decision because it was as if the defendants had unlawfully taken a file cabinet containing physical documents. *See id.* at 1278. Courts applying *Thyroff* thus have held that the “pure copying of electronic files without more” does not amount to conversion. *Fischkoff v. Iovance Biotherapeutics, Inc.*, 339 F. Supp. 3d 408, 414 (S.D.N.Y. 2018). A violation occurs only “when someone acts to block the interest holder from accessing his or her electronic data.” *Schatzki v. Weiser Capital Mgmt., LLC*, 2013 U.S. Dist. LEXIS 168572, at *40–41 (S.D.N.Y. Nov. 25, 2013). That is not the case here. The Court will dismiss Count XI.

4. *Count XII: Tortious Interference*

To state a tortious interference claim, a plaintiff must allege: “(1) an economic relationship between the plaintiff and some third party, with the probability of future economic benefit to the plaintiff; (2) the defendant’s knowledge of the relationship; (3) intentional acts on the part of the defendant designed to disrupt the relationship; (4) actual disruption of the relationship; and (5) economic harm to the plaintiff proximately caused by the acts of the defendant.” *Korea Supply Co. v. Lockheed Martin Corp.*, 63 P.3d 937, 950 (Cal. 2003) (internal quotation marks omitted); *see also Newmyer v. Sidwell Friends Sch.*, 128 A.3d 1023, 1038 (D.C. 2015) (similar).

Broidy's claim fails for the simple reason that the Complaint has not identified any "business relationship with a *specific* third party containing the probability of future economic benefit to the plaintiff." *Prostar Wireless Grp., LLC v. Domino's Pizza, Inc.*, 360 F. Supp. 3d 994, 1016 (N.D. Cal. 2018) (emphasis added) (internal quotation marks omitted); *see Sharpe v. Am. Acad. of Actuaries*, 285 F. Supp. 3d 285, 292 (D.D.C. 2018). A plaintiff's "general averment that it had relationships with its customers and prospective customers is insufficient." *Packaging Sys. v. PRC-Desoto Int'l, Inc.*, 268 F. Supp. 3d 1071, 1090 (C.D. Cal. 2017). Here, the Complaint merely alleges that Broidy had some undefined "business relationships" and that he had relationships with unidentified "Jewish clients." Complaint ¶¶ 363, 365. This is insufficient even at the pleadings stage. The Court will dismiss count XII.

5. *Count XIII: Civil Conspiracy*

"Conspiracy is not a cause of action, but a legal doctrine that imposes liability on persons who, although not actually committing a tort themselves, share with the immediate tortfeasors a common plan or design in its perpetration." *Applied Equip. Corp. v. Litton Saudi Arabia Ltd.*, 869 P.2d 454, 457 (1994) (en banc). "By participation in a civil conspiracy, . . . a coconspirator incurs tort liability co-equal with the immediate tortfeasors." *Id.*

To plead a civil conspiracy, a plaintiff must allege: "(1) formation and operation of the conspiracy and (2) damage resulting to plaintiff (3) from a wrongful act done in furtherance of the common design." *Rusheen v. Cohen*, 128 P.3d 713, 722 (Cal. 2006). The sufficiency of the pleadings "often turns upon the existence of an agreement, which is the essential element of a conspiracy claim." *Mattiaccio v. DHA Grp., Inc.*, 20 F. Supp. 3d 220, 230 (D.D.C. 2014) (internal quotation marks omitted). Direct evidence of such an agreement is rare in civil conspiracy cases. *Rawlings v. District of Columbia*, 820 F. Supp. 2d 92, 106 (D.D.C. 2011). Hence, one "may be inferred from the nature of the acts done, the relation of the parties, the

interests of the alleged conspirators, and other circumstances.” *Novartis Vaccines & Diagnostics, Inc. v. Stop Huntingdon Animal Cruelty USA, Inc.*, 50 Cal. Rptr. 3d 27, 35 (Ct. App. 2006) (internal quotation marks omitted); see *Halberstam v. Welch*, 705 F.2d 472, 486 (D.C. Cir. 1983).

The totality of the circumstantial evidence alleged plausibly supports a conspiracy claim. Broidy was an outspoken critic of Qatar. Complaint ¶ 1. All parties were retained by Qatar to engage in a public relations effort aimed at influencing the Trump Administration’s position on Qatar. *Id.* ¶¶ 50–51. “Muzin admitted that he identified and described Mr. Broidy to the Qatari government as an impediment to Qatar’s foreign policy interests in the United States.” *Id.* ¶ 73, 75. He further stated that Broidy’s name came up “often” in his weekly meetings at the Qatari embassy, *id.*, and that “everyone he ‘fingered’ was ‘in danger,’” *id.* ¶ 184. The Qatari Enterprise allegedly hired cyberhackers to target Broidy. *Id.* ¶ 78–106. Allaham texted Muzin on March 13, 2018 that Benomar went to Qatar “to get the emails” and Muzin responded by referencing Broidy by name. *Id.* ¶ 111. Before and during the period in which the articles referencing the hacked materials were published, Howard had an extensive string of calls with the publishers and members of the alleged Qatari enterprise, including some calls a mere two days after the hack. *Id.* ¶¶ 115–37. In the days leading up to one reporter declaring that he had received a new batch of emails, Howard exchanged several phone calls with him. *Id.* ¶ 128. On January 25, shortly after the hacking, Muzin sent Allaham a text stating, “It’s very good. . . . We got the press going after Broidy. I emailed you.” *Id.* ¶ 140. Muzin admitted to having foreknowledge of impending media stories and seems to have received this information from Howard. *Id.* ¶ 145–46, 174–79. On March 13, Muzin remarked to Allaham that recently published news stories about Broidy “[p]ut[] him in [M]ueller[’s] crosshairs.” *Id.* ¶ 147. Muzin told Allaham on May 4 that “our new

friends can make Broidy go away altogether.” *Id.* ¶ 159. Muzin and Allaham were paid by Qatar amounts which “far exceed[ed] the prevailing market rates for lobbying or political action.” *Id.* ¶ 169. Muzin received a pay raise from Qatar that coincided with the timing of the cyber hack. *Id.* ¶ 165. And “[w]hen Mowbray told Muzin that he suspected Muzin had helped initiate the cyber operation against Mr. Broidy, Muzin stated, ‘I was doing my job.’” *Id.* ¶ 187. Muzin then stated that “he needed ‘to be a little more careful’ when he spoke to Mowbray, and when Mowbray asserted that “Muzin was ‘neck deep in this conspiracy against Mr. Broidy, Muzin replied, ‘I know.’” *Id.* At the pleadings stage, these combined allegations withstand a motion to dismiss, and the defendants’ motion as to Count XIII will be denied.

F. First Amendment Defense

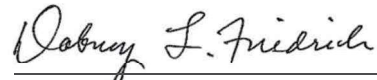
Howard urges that “even crediting the Complaint’s allegations that Howard received hacked emails and disseminated them to reporters,” the First Amendment shields him from liability because he did not personally hack Broidy’s servers and because “the Broidy emails embody a matter of great public concern.” Howard’s Mot. to Dismiss at 56. Though Howard is correct that Broidy does not allege Howard hacked the servers personally and that the articles do embody a matter of public concern, his argument is unavailing because he plausibly conspired with the hackers.

Howard relies principally on *Bartnicki v. Vopper*, 532 U.S. 514 (2001), a case in which the Supreme Court held that “a *stranger*’s illegal conduct does not suffice to remove the First Amendment shield from speech about a matter of public concern.” *Id.* at 535 (emphasis added). But unlike here, that case involved a reporter who “played no part in the illegal interception” of information he later obtained and published “in a manner lawful in itself but from a source who ha[d] obtained it unlawfully.” *Id.* at 525, 528. This case is different. Howard “is alleged to have

conspired with” the hackers and to have taken part in a scheme to disseminate the knowingly hacked information to the media. *See Cockrum v. Donald J. Trump for President, Inc.*, 365 F. Supp. 3d 652, 657 (E.D. Va. 2019). In a conspiracy, “[i]t is settled that an overt act of one partner may be the act of all.” *Pinkerton v. United States*, 328 U.S. 640, 646 (1946). Thus, if Broidy can establish Howard’s involvement in the conspiracy, Howard would be liable for the illegal interception as if he committed the hacking himself. The Court rejects Howard’s First Amendment defense.

CONCLUSION

For the foregoing reasons, the Court grants the defendants’ motions to dismiss as to Counts I (RICO), II (RICO conspiracy), III (Stored Communications Act), VIII (California Comprehensive Computer Data Access and Fraud Act), IX (public disclosure of private facts), XI (conversion), and XII (tortious interference). The Court denies the defendants’ motions to dismiss as to Counts IV (Computer Fraud and Abuse Act), V (Defend Trade Secrets Act), VI (California Uniform Trade Secrets Act), VII (receipt and possession of stolen property), X (intrusion upon seclusion), and XIII (civil conspiracy). A separate order consistent with this decision accompanies this memorandum opinion.


DABNEY L. FRIEDRICH
United States District Judge

March 31, 2020